제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

무선 인터넷 환경에서 컨텐츠 저작권 보호를 위한 모바일 보안시스템의 설계 및 구현

김 후종
국민대학교 전자공학과
e-mail : hjkim2@sktelecom.com

Design and Implementation of Mobile Security System for Content Rights Management in Wireless Internet Environment

Hoojong Kim

요 약

무선 인터넷이 활성화되면서 다양한 형태의 무선 컨텐츠가 상용화되고 있으며, 이와 동시에 불법적인 컨텐츠의 유통이 성행하게 되어 컨텐츠 보안을 위한 디지털 저작권 관리(DRM: Digital Rights Management)시스템이 요구되고 있다.

본 논문에서는 무선 인터넷 환경에서 유통되는 디지털 컨텐츠의 저작권 보호를 위한 모바일 보안 시스템을 제안하였다. 특히, 본 시스템에서 단말의 처리 능력을 고려하여 컨텐츠 부분 암호화 기법을 적용하여 신속한 복호화 수행이 가능하도록 설계하였다. 본 시스템을 적용할 경우 컨텐츠의 권리보호는 물론이며, 제한적인 모바일 디바이스에서 기존보다 신속한 수행이 가능해지는 효과를 기대할 수 있다

1. 서론

무선 인터넷 사용자의 증가와 함께 다양한 컨텐츠가 무선 인터넷 환경에서 디지털 형태로 제작되어 활발하게 유통되고 있다. 이와 같은 과정에서 디지털 컨텐츠의 불법 유통으로 인한 저작권 침해의 문제가 발생하고 있으며, 이러한 문제를 해결하기 위해서 디지털 저작관리(DRM: Digital Rights Management)기술의 필요성이 대두되고 있다[2]. DRM 기술은 컨텐츠를 유통, 관리하는 시스템으로써 유선뿐 아니라 무선에서도 다양한 비즈니스 모델을 지원하고 컨텐츠에 대한 접근이 용이해야 하고 암호화, 워터마킹 기술등을 사용하여 불법 사용을 억제하는 효율적인 인터넷 상거래 시스템으로 동작하여야 하는 기본적인 특징을 가진다[7].

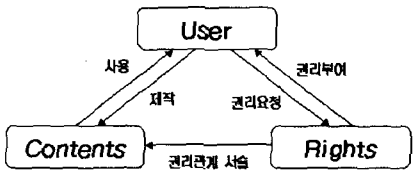
본 논문에서는 무선인터넷 환경에서 제공되는 디지털 컨텐츠를 보호하기 위한 모바일 보안 시스템을 제안하고자 한다. 특히, 무선 단말기의 성능을 고려하여 컨텐츠의 부분 암호화의 방법을 기존의 전체 암호화 방법과 성능 비교를 통해서 속도의 우수성을 검증하였다.

본 논문의 구성은 2장에서 일반적인 DRM 기술 및 무선인터넷 보안 기술을 서술하였고, 3장에서는 무선 환경에 적합한 모바일 보안시스템을 부분 암호화 기법으로 설계를 제안하였다. 4장에서는 프로토타입을 통한 성능 분석으로 테스트 결과를 나타냈으며, 마지막으로 5장에서는 결론과 향후 연구방향에 대해서 기술하였다.

2. 관련연구

2.1 DRM 기술현황

보안 기술은 인터넷에서 유통되고 있는 디지털 컨텐츠의 저작권을 보호하기 위한 기술로써 컨텐츠 암호화에 기반한 DRM 기술과 디지털 워터마킹(Didital Watermarking)기술등으로 적용되고 있다[1][3]. 워터마킹 기술은 소극적인 형태의 저작권 추적 기술이며 변조등 각종 공격에 취약하기 때문에 컨텐츠의 판매등 적극적인 권리 행사를 하기에는 적합하지 못하다는 의견이 있다. 반면에 DRM 기술은 컨텐츠의 저작권 소유자, 사용권 소유자, 사용기간, 사용 횟수등 보다 적극적이고 다양한 정보를 다룰 수 있고 강력한 복제 방지 기능을 지니고 있어서 최근 암호화를 위한 기술로써 웹 환경에서 활발하게 적용되고 있다. 일반적인 DRM의 구성 요소는 그림1과 같다[7].



<그림 1> DRM의 구성요소

사용자(User)는 원하는 컨텐츠(Contents)를 이용하기 위해서 컨텐츠 사용 권한에 대한 권리(Right)를 부여

받는다. 이때 권리의 의미는 컨텐츠에 관계된 소유, 사용, 변조, 배포 등 여러 가지 권리 관계를 서술하고 있다.

2.2 무선 인터넷에서의 보안 연구

유선 인터넷 보안의 경우는 Telnet, Ftp 등과 같이 원격지의 시스템을 사용하거나 원격지에 있는 자료를 사용하는 것으로 시작하여 침입차단 시스템, 침입탐지 시스템과 같은 네트워크 시스템 등을 대상으로 보안을 적용하고 있다. 반면에 무선 인터넷의 경우는 모바일 커머스, 모바일 뱅킹, 모바일 트레이딩과 같은 전송되는 데이터에 대한 보안 서비스가 먼저 요구되었다. 이로 인하여, 현재 무선 인터넷의 보안은 크게 W-PKI(Wireless Public Key Infrastructure), M-VPN(Mobile Virtual Private Network)시스템으로 적용되고 있다. 주요 특징은 [표 1]과 같다[4].

[표 1] 무선 인터넷 보안 특징

항목	W-PKI	M-VPN
응용 프로그램	불특정 다수에게 서비스하는 보안	특정 다수에게 서비스하는 보안
보안 측면	네트워크 보안 취약	네트워크와 전송 데이터의 완벽한 보안 서비스 적용
적용 규모	대규모의 응용 서비스	특정 사용자를 위한 규모의 응용 서비스
보안 정책 측면	신규 보안 정책 설정 필요	기존의 보안 정책 적용
신규시스템 측면	W-PKI 신규 시스템 필요	기존의 VPN 기술을 이용 (기술적 이해 용이)
응용 프로그램 관계	응용프로그램마다 연동 필요	응용 프로그램과 독립적 특성
비용 측면	고가	중가

3. 모바일 보안시스템 설계

본 절에서는 PDA(Personal Digital Assistants)를 대상으로 하는 컨텐츠 사용 권리에 대한 보안 시스템으로 부분 암호화 적용 설계 방법을 제안하였다.

3.1 시스템의 개요

본 시스템은 PDA에서 무선 인터넷 사용시 유통되고 있는 컨텐츠를 보호하기 위한 디지털 저작권 관리시스템(DRM: Digital Rights Management)을 부분 암호화 방법으로 제안하고자 하며 전체적인 시스템 구성도는 그림 2와 같다.

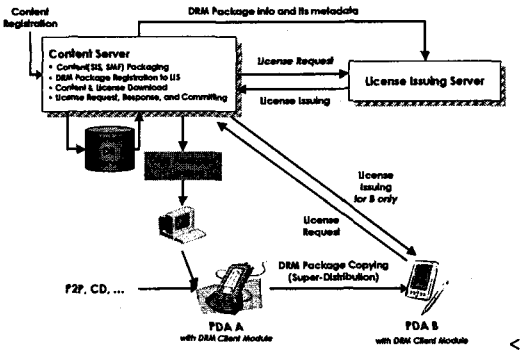


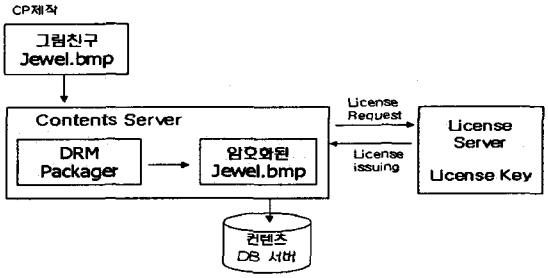
그림 2> 모바일 DRM의 시스템 구성도

3.2 컨텐츠 암호화 시스템의 설계

컨텐츠의 DRM 암호화의 인코딩 작업은 컨텐츠 서버와 라이센스 서버에서 이루어진다. 그 세부 설계는 다음과 같다.

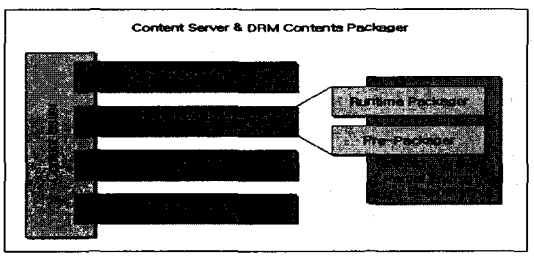
3.2.1 컨텐츠 서버의 암호화 설계

컨텐츠 서버에서는 CP(Contents Provider)가 제작한 이미지 파일 컨텐츠를 사례로 하였으며 암호화 패키징 도구를 통해서 DRM 컨텐츠가 완성되는 과정을 설명하면 그림 3과 같다.



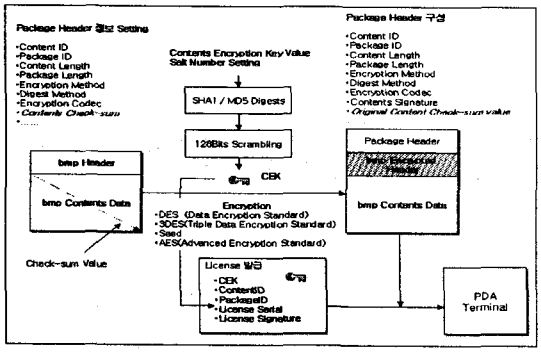
<그림 3> 컨텐츠 서버에서 암호화 과정

그림3에서 암호화 패키징 도구인 DRM Packager로 그림친구 원본 컨텐츠를 암호화 패키지로 재생성하는 과정이다. 이를 DRM Content Server 구조와 Contents Server Contens Packaging Tool의 구조를 관련지어서 설계하면 그림 4와 같다.



<그림 4> DRM Packager의 구조

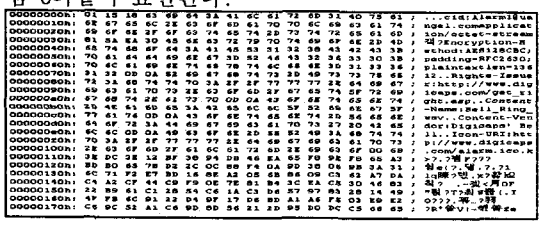
이때, 부분 암호화는 컨텐츠의 헤더 파일 영역을 암호화하고 컨텐츠 영역에서 필요 부분만 추출하여 암호화 하는 방법으로 그림 5의 구조를 보인다.



<그림 5> 부분 암호화 생성과정

부분 암호화와 전체 암호화와의 차이점은 헤더 부분과 컨텐츠의 Check-sum Value값을 측정하여 Encrypted Header에 반영하는 사항이다.

이와 같은 개념으로 패키징된 컨텐츠의 DRM Contents Header Sample을 추출하였으며 결과는 그림 6과같이 표현된다.

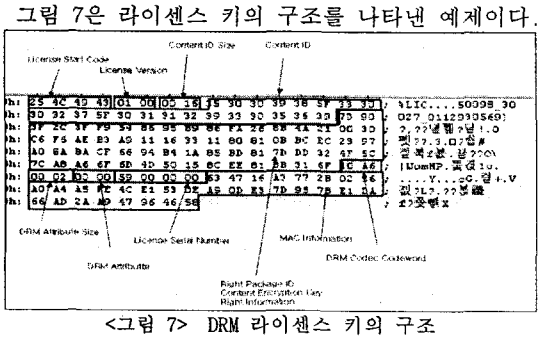


<그림 6> DRM Content Sample Hex View

3.2.2 License Server의 라이센스 발급 설계

라이센스 서버에서는 컨텐츠 서버에 새롭게 생성된 컨텐츠와 매핑되는 라이센스를 생성하고 컨텐츠 사용을 요청하는 PDA에 라이센스를 발급하는 기능을 담당한다. 라이센스 내의 데이터는 크게 해당 DRM Contents의 식별을 위한 정보와, 암호화된 DRM Contents의 CEK, DRM Content 사용의 제한을 둘 수 있는 Permission 및 Constraint 정보, 그리고, DRM Content의 Signature(전자서명) 정보를 담고 있다.

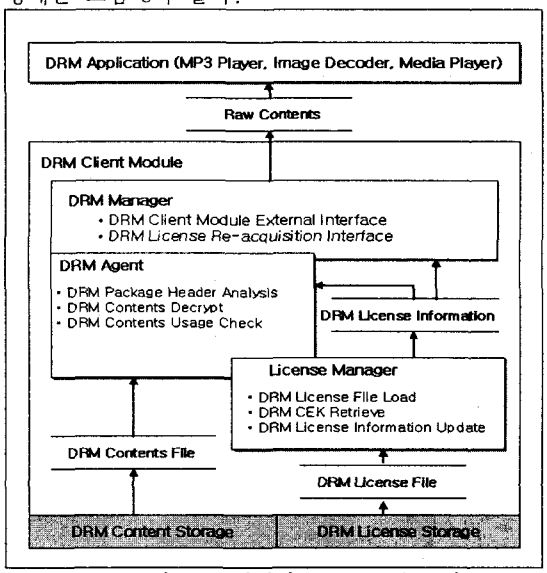
그림 7은 라이센스 키의 구조를 나타낸 예제이다.



<그림 7> DRM 라이센스 키의 구조

3.2.3 디바이스에서의 컨텐츠 복호화 설계

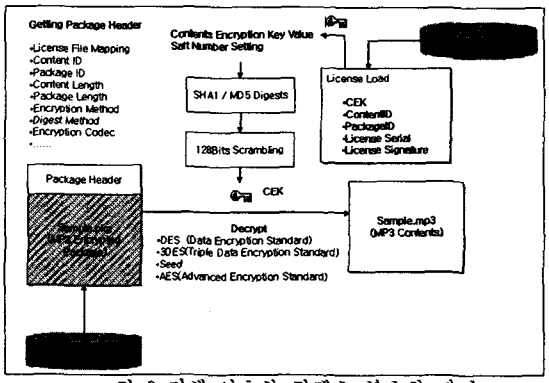
PDA에서는 컨텐츠를 다운받아 수행할 경우 암호화된 컨텐츠와 동시에 라이센스를 다운받게 된다. 암호화된 DRM 컨텐츠를 Playing, Viewing, Printing 그리고 Executing 하기위한 Player 및 Application은 DRM Client Module로부터 DRM 컨텐츠의 입/출력을 요청한다. 이와 같은 기능을 수행하는 클라이언트 모듈을 3개의 영역으로 나누어서 설계하였으며 형태는 그림 8과 같다.



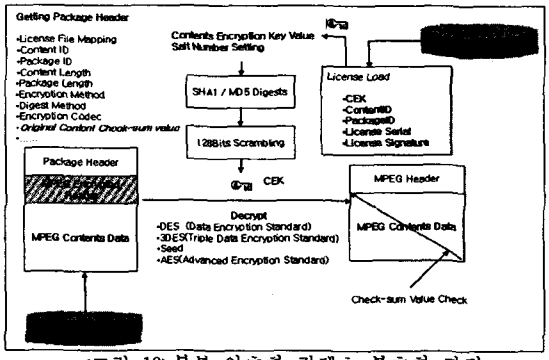
<그림 8> 클라이언트 DRM 모듈 구성

그림8에서 첫째, DRM Manager는 DRM Application에서 암호화된 컨텐츠의 DRM 패키지를 사용하고자 할 경우에 PDA에 내장된 Player 또는 Viewer에게 DRM 패키지에 대한 인증 및 접근과 사용에 대한 인터페이스를 제공한다. 둘째, DRM Agent는 DRM Manager로부터 요청 사항을 전달 받아 DRM 패키지에 대한 활용 여부를 확인하고 암호화된 DRM 컨텐츠를 복호화 처리한다. 셋째, License Manager는 DRM 패키지에 대한 라이센스를 관리하는 모듈로 라이센스 파일로부터 CEK를 추출하여 DRM Agent에 전달하며 DRM Agent 또는 DRM Manager의 요청에 따라 보유하고 있는 라이센스 리스트를 조회하고 사용하고자 하는 DRM 패키지의 라이센스에 대한 사용 횟수, 기간 등 사용 권한의 조회 및 변경 작업을 수행한다. 또한 라이센스 정보는 불법적인 복제 및 변경을 방지하기 위해 레지스트리에 정보를 저장하고 관리하게 된다

그림 9는 전체 암호화되어 있는 DRM 컨텐츠를 복호화 하기위한 처리 과정이고, 그림 10은 부분 암호화되어 있는 DRM 컨텐츠를 복호화 하기위한 처리의 비교 과정이다.



<그림 9>전체 암호화 컨텐츠 복호화 과정



<그림 10>부분 암호화 컨텐츠 복호화 과정

패키지 헤더에 구성될 Check-sum Value값의 적용 여부가 전체 암호화와 부분 암호화가 적용된 DRM컨텐츠에 대한 복호화의 차이를 나타내는 기준이다.

4. 구현 및 실험결과

본 논문에서 제안한 모바일 보안 시스템을 구현하기 위한 프로토타입의 개발 환경과 적용 후의 실험 결과는 다음과 같다.

4.1 개발환경

1) 모바일 디바이스 : PDA
2) 운영체제 : PPC2002(WinCE 계열)
3) 개발언어 : eVC++
4) Crypto 알고리즘 : SEED
5) 측정대상: Size별 이미지 File 의 컨텐츠 복호화 Time Tick Count

4.2 실험결과

실험결과는 전체 암호화와 부분 암호화에 따른 DRM 컨텐츠를 WinCE 계열의 운영체제를 사용하고 있는 POZ에서 복호화 수행된 처리 속도를 비교하여 표 2와 같이 나타내었다. 즉 복호화 수행 속도는 암호화된 컨텐츠의 블록 사이즈에 비례하는 결과를 보였다. 따라서 전체 암호화된 컨텐츠를 복호화 처리하는 것보다는 동일한 사이즈의 헤더만을 부분적으로 처리한 컨텐츠를 복호화하여 처리할 경우 현저한 속도의 개선을 표 2와 같이 보여주었다.

[표2] 복호화 수행 결과

Test 단말기	서비스	Algorithm	Test File	Size(Bytes)	Time(ms)	
					전체복호화	부분복호화
POZ	그림친구 서비스	SEED	10K Image	10,909	130	11.2
			20K Image	19,581	148	12.2
			30K Image	30,973	267	11.7
			40K Image	42,877	204	12.1
			50K Image	55,437	234	12.2
			60K Image	64,781	276	11.5
			70K Image	75,661	285	11.3
			80K Image	80,989	331	11.2
			90K Image	95,853	333	12.2
			100K Image	119,534	395	11.5
			200K Image	194,318	613	11.5
			300K Image	299,166	559	11.6
			500K Image	486,334	1293	12.0
			1000K Image	1,089,727	2816	11.8

5. 결론

본 논문에서는 무선 인터넷에서 유통되고 있는 디지털 컨텐츠의 저작권을 보호하기 위해서 DRM이 적용된 모바일 보안 시스템의 설계를 제안하였다. 특히 부분 암호화를 통한 설계 시스템으로 기존보다 디바이스에서 컨텐츠의 수행속도 개선의 효과를 확인할 수 있었다.

향후의 연구 계획은 본 논문에서 제안한 DRM 설계 방법을 고도화하고 처리 능력이 제한적인 터미널에서 원활한 수행이 가능한 복호화 가속기의 개발을 추가로 연구하여, 휴대폰이나 기타 다른 디바이스에 적용할 계획이다.

참고문헌

[1]Joshua, D. Susan, K, "Understanding DRM System" An IDC White Paper", IDC, 2001.
[2]권순홍, "실시간 멀티미디어 서비스의 DRM 적용방법 설계", 정보과학회 춘계학술대회, VOL.29, NO.01, pp. 0481~0483, 2002.04.
[3]박주상, "Microsoft의 디지털 저작권 보호 기술 분석 및 향후 시스템 개발 요소", 정보처리학회 추계학술대회, Vol.9, No.02, 2002. 10.
[4]윤감규 역자, 전자보안시스템, 동일 출판사, 1996.12.
[5]이용호, "에이전트 기반의 동적 디지털 저작권 관리 시스템 설계 및 구현", 한국정보처리학회 논문지 D, VOL.08, NO.05, pp. 0613~0622, 2001.10.
[6]정재권, 류대길, 강한 공역, 보안과 암호화, 인포북, 2001. 6.
[7]한국 디지털 콘텐츠 포럼, 디지털 유통 프레임 워크 구축 및 기술표준 전략 수립에 관한 연구, 2002. 2.